

## REMARKS

Reconsideration of the subject application is amended herein is respectfully requested.

The Examiner has rejected claims 1-4, 6-9 as being obvious over Wasilewski in view Atkinson. Neither of these references were previously cited. The Applicants respectfully traverse this rejection. Claim 1 expressly recites a method of transporting packets between a subscriber specific access interface and the concentration router of a shared network. Moreover, the claim further recites that police control operation are carried out at the subscriber specific access interface, for generic IP traffic directed from the subscriber installations toward the concentration router. Wasilewski does not disclose such a method or system.

The Examiner considers the service access and broad band encrypter remapper (SABER) or the conditional access manager (CAM) as corresponding to the access interface of the present invention. However, as becomes clear when reviewing paragraph 0036 of the subject reference, SABER or CAM are not subscriber installation specific. This is also clear from Figure 2, where the set top units (STUs) correspond to the subscriber installations. In Figure 2, there are a plurality of STUs but only one SABER and CAM. Furthermore, the SABER and CAM are physically located on the service provider's side and these elements are connected through network operator's digital network and network access nodes (NANs) to the STUs. It is also to be noted that the service providers cannot be

considered as being subscribers. In the solution of Wasilewski the STUs are customers and therefore subscribers to the service providers.

Moreover, the policy operations described in Wasilewski apply to multimedia traffic directed from the service provider content servers towards subscribers, and relate only to encryption/decryption of such streams, while our invention relates to generic (not only multimedia) traffic directed from subscriber to network (i.e. reverse direction), and the policy regards also this direction, in addition of being generic, not only related to encryption.

The aim of the Wasilewski is to allow the service providers to ensure that programs entering the digital network are viewed only by the customers (STUs) that have been authorized by a server gateway of the service provider. Wasilewski thus provides a solution to provide conditional access to programs before those programs enter the digital network.

Furthermore, in the solution of Wasilewski, packets are transmitted from the network operator's network to customers, whereas in the present invention the situation is opposite, i.e. packets are transmitted from the customers to the concentrating router.

Thus, the aim of Wasilewski is quite distinct from the present invention. The aim of the present invention is to provide a mode of operation of the network which enables a wide diversity of stream controls to be taken into account without resulting in an excessive increase in the complexity of the concentrating routers, and with a flexibility of configuration (page 2, lines 27-32).

The solution provided by Wasilewski is not flexible since the subscriber has no easy way or perhaps no means at all of adjusting the configurations of SABER and CAM. Even if in the solution of Wasilewski the concentrating routers (NANs) are not necessary complicated, the SABER and the CAM still remain complicated.

As already stated in previous submissions by the Applicants, the fact that the access interface is subscriber installation specific has clear technical advantages. The stream control operations pertaining to the contractual framework between the manager of the network and the subscriber are thus decentralized, thereby avoiding the need for the concentrating router to take on all diversity of the operations demanded by the various subscriptions (page 3, lines 15-20).

Moreover, the subscriber benefits from greater flexibility for dynamically defining the characteristics of his subscription. He merely needs to intervene at the level of the access interface with which he is furnished. He may also define the control functions pertaining to the contractual framework with the access provider on the same platform as the other control functions which he uses for the internal organisation of his installation, thereby simplifying organisation thereof (page 3, line 15 - page 4, line 4). These advantages cannot be achieved by the solution provided by Wasilewski. Furthermore the claimed elements discussed above are absent from the other references as well.

These arguments also apply to the corresponding independent access interface claim (claim 6) and claims dependent thereon. Based on the foregoing,


the above-identified features are not disclosed or rendered obvious by Wasilewski even with combination with the other cited art.

In summary, it is respectfully submitted that the subject application is patentably distinguishable and therefore it should be allowed.

Respectfully submitted,

**GOTTLIEB, RACKMAN & REISMAN, P.C.**

270 Madison Avenue  
New York, NY 10016-0601  
Telephone: (212) 684-3900  
Facsimile: (212) 684-3999

---

Tibor Weisz, Esq.  
Reg. No. 29,876

Dated: May 21, 2007